IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/846,175
Filing Date 4/30/2001
Inventorship ..... Brezak et al.
Applicant ..... Microsoft Corp.
Group Art Unit 2135
Examiner ..... Son, Linh L.D.
Attorney's Docket No. ms1-646us
Title: "Methods and Arrangements For Controlling Access To Resources Based on Authentication Method"

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Lance Sadler (Tel. 509-324-9256x226; Fax 509-323-8979)
Customer No. 22801

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/846,175, filed April, 30, 2001, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-26 stand rejected and are pending in the Application. The claims are set forth in the Appendix of Appealed Claims on page 15.

(4) Status of Amendments

A final Office Action was issued on May 3, 2006.

Claims 1, 5, 11, 15, 21, 25 and 26 were amended responsive thereto in a paper dated June 30, 2006.

An Advisory Action issued July 20, 2006 from which this appeal is taken.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters, if any. These specific reference characters are examples of particular elements of the drawings for

certain embodiments of the claimed subject matter and the claims are not limited to solely the elements corresponding to these reference characters.

With regard to claim 1, a method for use in a computer capable of supporting multiple authentication mechanisms comprises generating at least one indicator (110, Fig. 1) that identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user (Page 7, lines 6-14; Fig. 1, 110), wherein generating the indicator (110, Fig. 1) further includes identifying within the indicator (page 3, lines 19-23) at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism (page 6, line 22 – page 7, line 5); and controlling the user's access (page 8, lines 3-13) to at least one resource based on the indicator.

With regard to claim 11, a computer-readable medium for use in a device capable of supporting multiple authentication mechanisms has computer-executable instructions for performing acts comprising producing at least one indicator (110, Fig. 1) that identifies a user, and uniquely identifies at least one authentication mechanism supported by the device that has been used to authenticate the user (Page 7, lines 6-14; Fig. 1, 110), wherein producing the indicator further includes identifying within the indicator (page 3, lines 19-23) at least one characteristic of the authentication mechanism, wherein the at least one characteristic of the authentication mechanism includes a strength characteristic of the authentication mechanism (page 6, line 22 – page 7, line 5); and causing the

device to selectively control the user's access (page 8, lines 3-13) to at least one resource operatively coupled to the device based at least in part on the indicator.

With regard to claim 21, an apparatus comprises at least one authentication mechanism configured to generate at least one indicator (110, Fig. 1) that identifies a user, and identifies the authentication mechanism that has been used to authenticate the user (Page 7, lines 6-14; Fig. 1, 110), wherein the indicator (110, Fig. 1) further includes at least one identifying characteristic associated with the authentication mechanism, wherein the at least one identifying characteristic associated with the authentication mechanism indicates a measure of strength of the authentication mechanism (page 6, line 22 – page 7, line 5); an access control list; at least one access controlled resource (page 8, lines 3-13); and logic operatively configured to compare the indicator with the access control list and selectively control the user's access to the resource based on the indicator.

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-26 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,052,468 to Hillhouse (hereafter "Hillhouse").

Before discussing the substance of the Office's rejections, the following discussion of Applicant's disclosure as well as the reference to Hillhouse is provided.

Applicant's Disclosure

Applicant's disclosure provides methods and arrangements for controlling access to resources in a computing environment. These methods and

arrangements identify authentication mechanism(s) (and/or characteristics thereof) used in verifying a user to subsequently operating security mechanisms. Thus, additional control is provided by differentiating user requests based on this ***additional information***. For example, in a computer capable of supporting multiple authentication mechanisms, at least one embodiment ***generates an operating system representation*** of at least one ***identity indicator*** associated with at least one authentication mechanism, and subsequently ***controls access*** (to at least one resource) ***based on the operating system representation***. In certain implementations, at least one security identifier that identifies the authentication mechanism in some way can be generated. In other implementations, the operating system representation is compared to at least one access control list (with at least one access control entry). Here, for example, the access control entry may specify ***whether the user authenticated (by the authentication mechanism) is permitted access to the resource***.

The Hillhouse Reference

Hillhouse discloses systems and methods for improving portability of secure encryption key data files by ***re-securing*** key data files according to different security processes for mobility.

Specifically, Hillhouse teaches a method of generating secure key databases that is portable to systems having different configurations. Hillhouse also teaches a ***method of selecting a user authentication method from a plurality of user authorization methods for use in securing*** a key data file. Finally, Hillhouse teaches a method of ***securing*** a key database with multiple security methods.

In accordance with Hillhouse's teachings, a key data file comprises a secured cryptographic key which can be secured again according to an authentication method selected from a plurality of available authentication methods available to a user on a particular system. Additionally, the key can be ***re-secured*** over and over again based on selected available authentication methods. The key data is then accessible only via the authentication method(s) used. Thus, the systems and methods in Hillhouse ***control access to key data files by securing a cryptographic key to that file.***

(7) Argument

A. The § 102 rejection of claims 1-26 over Hillhouse should be withdrawn.

Claims 1, 2, and 5-10

Claim 1 recites a method for use in a computer capable of supporting multiple authentication mechanisms, the method comprising [emphasis added]:

- generating at least one indicator that ***identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user***, wherein generating the indicator further includes identifying within the indicator at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism; and
- controlling the user's access to at least one resource based on the indicator.

In making out the rejection of this claim, the Office argues that Hillhouse discloses generating at least one indicator associated with and identifying at least one authentication mechanism that has been used to authenticate a user (citing column 8 lines 27-43 and Column 1, lines 35-45) and controlling access to at least one resource based on the indicator (citing column 1, lines 35-45, column 5 lines 32-38, and column 8 lines 35-43).

In addition, in the Advisory Action dated July 20, 2006, the Office further argues that the recited indicator is disclosed in Hillhouse in column 8, lines 30-35. Still further, the Office further argues that "the authentication mechanism uses to authenticate for access data. For instance, a user can select a number of authentication methods...as the authentication mechanism to secure data." (citing to column 7, lines 30-35) The Office argues that the indicator of a user authentication method is a 2 byte indicator, unique to each available method and that the strength characteristic is directly explanatory by its authentication method. Further, the Office states the "indicator of authentication method is directly explicit the authentication method characteristic of strength."

Applicant disagrees and traverses the Office's rejections.

This claim recites generating at least one indicator ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism ***that has been used to authenticate the user, and controlling the user's access to at least one resource based on the indicator.***

The excerpt cited by the Office at column 8, lines 27-43, merely discusses a method in which code two bytes in length ***indicates the type of authentication method*** (i.e., fingerprint, password, etc.) that must be used in order to gain access

to a key file comprising a cryptographic key. The indicator does not indicate that the user ***has been*** authenticated. This excerpt from column 8 is reproduced below:

> According to one embodiment the data indicative of a user authorization method comprises a sequence of bytes including a length for indicating, one of the data length and the number of authentication methods employed to secure the key data ***and an indicator of a user authentication method comprising a number, for example 2 bytes, unique to each available method***. Typically two bytes are used to identify the method selected thereby allowing for over 65,000 different user authentication methods. ***This permits the implementation of variations on user authentication methods to increase the difficulty of breaking the security of the key data.***

There is simply no disclosure or suggestion of an indicator that ***identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user***.

This excerpt is perhaps best understood when read in the context of the text that appears around it. Specifically, an excerpt from column 7, line 65 through column 8, line 44 is provided just below:

> In accordance with the invention, a method is provided to provide secure access to encrypted data by each of a plurality of people. Accordingly, ***a user determines to secure a key data file*** comprising a secured cryptographic key. The user is authenticated and the cryptographic key is accessed. ***The user selects an authentication method*** in the form of a biometric authentication method such as a fingerprint, a voiceprint, a face, a palm print, a retinal scan, and so forth; a password; or a key. The authentication method is selected from a plurality of available authentication methods. ***Another user is authenticated according to the selected method and the secured cryptographic key is secured according to that method***. The secured cryptographic key is stored in a second other key data file with data relating to the selected authorisation method. Alternatively, the key data is stored in a same file along with the previous secure key data. This allows for user authentication of any of a plurality of individuals providing access to same key data.

In some systems, a key data server comprises secure key data for a plurality of cryptographic keys. Using such a system and prior to travel, a user requests packaging of some keys for transport. The keys are packaged on a non-volatile memory device in the form of a smart card, a floppy disk, a PCMCIA card, a dongle, or another similar device. Prior to packaging the keys are secured according to a user selected authorisation method. The key server accesses the key data and then secures it according to the selected method and stores the resultant key data file and data indicative of the selected method in the non-volatile memory device.

According to an embodiment ***the data indicative of a user authorisation method comprises a sequence of bytes including a length for indicating, one of the data length and the number of authentication methods employed to secure the key data and an indicator of a user authentication method*** comprising a number, for example 2 bytes, unique to each available method. Typically two bytes are used to identify the method selected thereby allowing for over 65,000 different user authentication methods. This permits the implementation of variations on user authentication methods to increase the difficulty of breaking the security of the key data. Preferably only a single byte is used to indicate data length as it is obvious to those in the art that requiring application of more than 128 methods of user authentication in order to access key data renders such a system inconvenient. Of course, when desired, such a configuration can be implemented without difficulty.

Hence, what is described above is not the notion of an indicator that identifies a user and which is associated with and identifies at least one authentication mechanism that *has been used* to authenticate the user. Rather, Hillhouse describes the notion of using an identifier to identify one of a number of authentication methods that *can* be used. As Hillhouse instructs, "[t]his permits the implementation of variations on user authentication methods to increase the difficulty of breaking the security of the key data."

Furthermore, the excerpt cited by the Office at column 8 lines 1-15 (reproduced above) merely teaches that one user may be authenticated and then

subsequently access a key and then select an authentication method that must be used by a second user in order to access the same key. The second user may only access the key after being authenticated by the method chosen by the first user.

Thus, while Hillhouse discloses an indicator that indicates the type of authentication method that must be used by the second user to access the key, there is no mention whatsoever in this excerpt of an indicator ***that identifies a user, and is*** associated with and ***identifies*** at least one authentication mechanism ***that has been used to authenticate the user, and controlling the user's access to at least one resource based on the indicator.***

Furthermore, the Hillhouse excerpt cited by the Office in the Advisory Action (Column 7, lines 30-35) in no way, shape or form discloses or teaches the subject matter of this claim. As an example, consider this excerpt (and surrounding material) just below:

> Referring to FIG. 5, a method is provided to secure encryption key data. Accordingly, a user determines to secure a key data file comprising a secured cryptographic key. The user selects an authentication method in the form of a biometric authentication method such as a fingerprint, a voiceprint, a face, a palm print, a retinal scan, and so forth. Alternatively, another authentication method such as a password or a physical key is selected. The authentication method is selected from a plurality of available authentication methods available to the user. The user is authenticated according to the selected method and the secured cryptographic key is secured again according to that method. The secured cryptographic key is stored in the key data file with data relating to the selected authorisation methods and an order of securing operations. The user then selects a further authentication method and the key data is again secured and so forth. Each user authorisation is temporarily stored. The user is also authorised to access the key data as secured prior to application of the method shown in FIG. 5. The key data is then accessed and secured in each permutation of the selected methods. In the example of FIG. 5, this involves securing the key data according to method (1, 2, 3) (1, 3, 2) (2, 1, 3) (2, 3, 1) (3, 1, 2) (3, 2, 1), in six different forms. The

resulting data is accessible by providing, in any order, the three appropriate user authentication information samples.

Again, there is no disclosure or suggestion of an indicator that ***identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user.*** Accordingly, for at least this reason, this claim is allowable.

Further, this claim recites "identifying ***within the indicator*** at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a ***measure of strength of the authentication mechanism.***

The Office argues in the Advisory Action that the strength characteristic is directly explanatory by its authentication method. Applicant respectfully submits that Hillhouse simply does not provide an indicator, as described above, which includes an identified characteristic that includes a measure of the strength of the authentication mechanism. This subject matter is simply missing from Hillhouse.

And, while certain authentication mechanisms may be stronger than others, as the Office suggests, Hillhouse simply does not disclose, teach or suggest an indicator that: (1) identifies a user, (2) is associated with and identifies at least one authentication mechanism that has been used to authenticate the user, (3) identifies at least one characteristic associated with the authentication mechanism, the characteristic including a measure of strength of the authentication mechanism, and (4) controls the user's access to at least one resource **based on** the indicator (which includes features (1), (2) and (3)). This subject matter is simply missing from Hillhouse.

Accordingly, for at least this additional reason, this claim is allowable.

Claims 2 and 5-10 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested by the reference of record.

Claims 11, 12, and 15-20

Claim 11 recites computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising [emphasis added]:

- producing at least one ***indicator that identifies a user, and uniquely identifies at least one authentication mechanism supported by the device that has been used to authenticate the user***, wherein producing the indicator further includes ***identifying within the indicator at least one characteristic of the authentication mechanism***, wherein the at least one characteristic of the authentication mechanism includes a ***strength characteristic of the authentication mechanism***; and
- causing the device to selectively control the user's access to at least one resource operatively coupled to the device based at least in part on the indicator.

In making the rejection of claim 11, the Office uses much the same argument as used in making out a rejection of claim 1. For the reasons set forth above with regard to claim 1, Applicant respectfully traverses the Office's rejections. Accordingly, this claim is allowable.

Claims 12 and 15-20 depend from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither shown nor suggested by the reference of record.

Claims 21, 22 and 25-26

Claim 21 recites an apparatus comprising [emphasis added]:

- at least one authentication mechanism configured to generate at least one ***indicator that identifies a user, and identifies the authentication mechanism that has been used to authenticate the user***, wherein the indicator further includes ***at least one identifying characteristic associated with the authentication mechanism***, wherein the at least one identifying characteristic associated with the authentication mechanism ***indicates a measure of strength of the authentication mechanism***;
- an access control list;
- at least one access controlled resource; and
- logic operatively configured to ***compare the indicator with the access control list and selectively control the user's access to the resource based on the indicator.***

In making out the rejection of claim 21, the Office uses much the same argument as used in making out a rejection of claim 1. For all of the reasons set forth above with regard to claim 1, Applicant respectfully traverses the Office's rejections. Accordingly, this claim is allowable.

Claims 22 and 25-26 depend from claim 21 and are allowable as depending from an allowable base claim. These claims are also allowable for their

own recited features which, in combination with those recited in claim 21, are neither shown nor suggested by the reference of record.

Conclusion

The Office has not established a prima facie case of obviousness. Accordingly, Applicant respectfully requests that the rejections be overturned and that the pending claims be allowed to issue.

Respectfully Submitted,

Dated: 10/27/06

By: _____

Lance R. Sadler
Lee & Hayes, PLLC
Reg. No. 38,605
(509) 324-9256 ext. 226

(8) Appendix of Appealed Claims

1. (Previously Presented) A method for use in a computer capable of supporting multiple authentication mechanisms, the method comprising:

generating at least one indicator that identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user, wherein generating the indicator further includes identifying within the indicator at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism; and

controlling the user's access to at least one resource based on the indicator.

2. (Original) The method as recited in Claim 1, wherein generating the indicator further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism.

3. (Canceled).

4. (Canceled).

5. (Previously Presented) The method as recited in Claim 1, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

6. (Original) The method as recited in Claim 1, wherein controlling access to the resource based on the indicator further includes comparing the indicator to at least one access control list having at least one access control entry therein.

7. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is allowed to proceed.

8. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is not permitted to access the resource, then access to the at least one resource is not allowed to proceed.

9. (Original) The method as recited in Claim 6, wherein if the access control entry does not operatively specify that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is not allowed to proceed.

10. (Original) The method as recited in Claim 1, wherein the indicator includes a security token.

11. (Previously Presented) A computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising:

producing at least one indicator that identifies a user, and uniquely identifies at least one authentication mechanism supported by the device that has been used to authenticate the user, wherein producing the indicator further includes identifying within the indicator at least one characteristic of the authentication mechanism, wherein the at least one characteristic of the authentication mechanism includes a strength characteristic of the authentication mechanism; and

causing the device to selectively control the user's access to at least one resource operatively coupled to the device based at least in part on the indicator.

12. (Original) The computer-readable medium as recited in Claim 11, wherein producing the indicator further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication

mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism, in response thereto.

13. (Canceled).

14. (Canceled).

15. (Previously Presented) The computer-readable medium as recited in Claim 12, wherein the strength characteristic identifies a length of an encryption key employed by the authentication mechanism.

16. (Original) The computer-readable medium as recited in Claim 11, wherein causing the device to selectively control access to the at least one resource based on the indicator further includes causing the device to compare the indicator to control data .

17. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data specifies that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is allowed.

18. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data operatively specifies that the authentication mechanism is not permitted to access the resource, to which subsequent access to the resource is prohibited.

19. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data does not operatively specify that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is prohibited.

20. (Original) The computer-readable medium as recited in Claim 10, wherein the indicator includes a security token.

21. (Previously Presented) An apparatus comprising:

at least one authentication mechanism configured to generate at least one indicator that identifies a user, and identifies the authentication mechanism that has been used to authenticate the user, wherein the indicator further includes at least one identifying characteristic associated with the authentication mechanism, wherein the at least one identifying characteristic associated with the authentication mechanism indicates a measure of strength of the authentication mechanism;

an access control list;

at least one access controlled resource; and

logic operatively configured to compare the indicator with the access control list and selectively control the user's access to the resource based on the indicator .

22. (Original) The apparatus as recited in Claim 21, wherein the authentication mechanism is further configured to receive user inputs and generate at least one security identifier (SID) that identifies the authentication mechanism based on the user inputs.

23. (Canceled).

24. (Canceled).

25. (Previously Presented) The apparatus as recited in Claim 21, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

26. (Previously Presented) The apparatus as recited in Claim 21, wherein the indicator includes a security token.

(9) Evidence appendix. None

(10) Related proceedings appendix. None